

NAVAL WAR COLLEGE
Newport, R.I.

THE COMING CRISIS IN CRISIS PLANNING

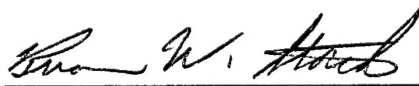
by

Brian W. Storck

Lieutenant Colonel, USAF

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

16 May 2000

Professor David F. Chandler

William J. Gibbons, COL, USMC

Special thanks to Captain Margaret Biewer, USAF, and the Information Warriors of the National Air Intelligence Center, Directorate of Intelligence Analysis

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DTIC QUALITY INSPECTED 4
20000912 123

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): THE COMING CRISIS IN CRISIS PLANNING (UNCLAS)			
9. Personal Authors: BRIAN W. STORCK, LT COL USAF			
10. Type of Report: FINAL		11. Date of Report: 16 MAY 2000	
12. Page Count: 18		12A Paper Advisor (if any): WALT WILDEMANN, CDR USN	
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: CRISIS, PLANNING, CINC, HEADQUARTERS, REACH BACK, TECHNOLOGY, INTERNET, OPSEC, KOSOVO, DECEPTION			
15. Abstract: Crisis planning at the CINC level is itself facing a crisis due to the pressures of an growing workload and rapid changes in technology. Multinational operations and new security challenges will increase the burden on crisis planners in the future. The Internet and other new communications technologies will radically change the environment in which military operations are planned and conducted. Augmentation, "reach back," and simplification will all provide some relief for future crisis planners. High-level interest is needed to encourage creative solutions to the problem.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

THE COMING CRISIS IN CRISIS PLANNING

Most staff officers are familiar with the planning drill at a regional CINC headquarters when a crisis erupts. The planning cell is formed, the maps go up on the wall, the computers and secure phones are checked out, and the fun begins. The mission is clarified, the best course of action is determined, and a plan is approved. After several days, weeks or months the crisis is resolved (or not) and the draftees in the crisis action team (CAT) are allowed to escape back to their "real" jobs. Regional CINC staffs have run this drill countless times in the past ten years, and the process has generally been successful, although painful. Unfortunately, current methods for conducting crisis planning are becoming obsolete -- indeed, the entire concept of doing crisis planning at the CINC level may be unworkable in a few years' time.

Too alarmist? Consider the following scenario: You are working as the J-35 of a very busy regional CINC headquarters about five years from today. Your boss, the J-3, calls to inform you the President is considering intervention in East Tarzania and the CINC has been ordered to present options ASAP. You have no Tarzanian experts on the staff, and many of your planners are already working other crises. Your plan must be pre-coordinated with three US military services, two US government agencies, five allied governments and six non-governmental relief organizations. The J-3 believes the NCA will want "something firm" within 24 hours. CNN is showing a live feed of atrocities on the streets of the Tarzanian capital; the PAO has just informed you that a news crew is at the front gate asking for you by name. Enjoy!

The validity of the unhappy scenario above rests on two major developments in the world around us: one is political in nature; the other, technological. The first development is the emergence of a fragmented post-Cold War world in which the US must often play the role of

policeman. The second development is the rapid emergence of information-sharing technologies, especially the Internet, which will radically transform the environment in which military operations are planned and conducted. Together, these two trends are rapidly making the current method of crisis planning at the CINC level less than satisfactory. Without prompt action to re-think current ways of doing the planning business and to assess the impact of new information technologies, the CINC crisis planning process will eventually fail.

A CRUSHING WORKLOAD

CINC staffs have always been busy, but during the past several years the crisis planning load on regional CINCs has grown especially heavy. Consider the case of US European Command (EUCOM), one of the busiest of the regional CINC headquarters in the 1990s. For example, during the period of 1991 to 1993, EUCOM was involved more than 21 contingencies which required major crisis planning efforts and stood up a CAT on the average of one every six weeks.¹ These operations ranged from small-scale US-only non-combatant evacuation operations (NEOs) in Africa to large-scale multinational efforts in the Balkans. At the same time, EUCOM planners were already handling the fallout of the collapse of the Warsaw Pact, dealing with a host of issues such as new military-to-military contact programs, NATO expansion and the spread of weapons of mass destruction (WMD). This blistering pace of operations continued throughout the 1990s.

To handle crisis planning actions, EUCOM resorted to the old trick of “robbing Peter to pay Paul.” Typically, action officers were removed from their normal directorate jobs and placed in a crisis action team (CAT) to handle crisis planning duties. Normal job functions were officially

¹ Robert Chelberg, Jack Ellertson, and David Shelley, “EUCOM - At the Center of the Vortex,” *Field Artillery*, October 1993, pp.12-16.

placed on hold until the crisis had passed (although some staffers cheated and tried to work two jobs at once.) Unfortunately, many so-called short duration CATs dragged on to the point where normal headquarters missions were severely impacted. "Beeper fatigue," burnout and low morale became a real problem in the headquarters staff. Eventually, HQ EUCOM compensated by bringing in large numbers of augmentees, including seconded personnel from CONUS units and reservists. This solution had its own problems in the form of increased training requirements, lack of continuity and excessive cost. Nonetheless, a permanent increase in the size of the EUCOM staff to handle the continuing workload was never possible. Congressionally mandated manpower ceilings in Europe and concerns about "bloated" headquarters put a significant increase in HQ EUCOM manning out of the question.

Regrettably, the CINC crisis planning workload is not expected to ease in the future. The US National Security Strategy is firmly wedded to a policy of selective engagement, and the bar seems to be dropping every year on what qualifies for military attention. As a recent example, on 29 April President Clinton announced that the worldwide AIDS epidemic was now being treated as a national security issue due to its potential for creating instability in many nations hard-hit by the disease.² It takes no great imagination to envision the raft of new crisis planning tasks in Africa which will fall upon the already hard-pressed EUCOM staff as a result of this decision. Similarly heavy crisis planning workloads can readily be projected for PACOM, SOUTHCOM and CENTCOM. The area of responsibility for each of the regional CINCs contains a large number of potential ethnic, political and economic flashpoints which have become increasingly prone to ignite since the restraints of the bipolar Cold War world have been removed. Barring a

² Barton Gellman, "AIDS Declared Threat to Security," *The Washington Post*, 30 April 2000, p. A1.

US return to an isolationist foreign policy, the forces commanded by regional CINCs will be very busy indeed in dealing with these brush fires. The CINC's crisis planners will be busier yet.

The obvious solution -- a significant, permanent increase in CINC planning staffs -- remains extremely unlikely. Senior DoD and military leadership is regularly stung by criticism from outside "experts" railing against overmanned headquarters and making simplistic "tooth-to-tail comparisons." More significantly, headquarters manning levels are also under pressure from the service staffs themselves. Faced with a requirement to fully man high op tempo deploying units, the services have often raided headquarters manning to provide the necessary personnel.

A recent example is the difficult Air Force transition to the new Air Expeditionary Force (AEF) structure. Requiring significant increases in manning at the wing level, the Air Force is reducing manning at Air Combat Command Headquarters by over 50 percent to help free up the necessary billets. The Air Staff itself is facing cuts of 20 percent over the next five years.

Although the Air Force (unlike the other services) had previously honored the requirement to man joint billets at 100 percent, in 1999 the Air Force enacted a policy to man joint positions at levels not exceeding USAF-wide fills.³ Given the continuing USAF shortfalls in field-grade manning (as low as 50-60% in some specialties), the impact on CINC staffs will be profound. The Navy, Marine Corps and Army are all facing similar joint manning challenges. Thus, CINC headquarters manning may actually decrease in future. Although near-term billet cuts at the CINC level are unlikely due to Congressional oversight, CINC planning staffs will inevitably suffer from a gradual drawdown of on-hand personnel, lower experience levels and lack of continuity as service-wide manning problems remain acute.

³ Air Force Personnel Center briefing, ACC Commanders' Orientation Course, Langley AFB, VA, March 20, 1999

THE EMERGENCE OF THE INFOSPHERE

The work environment of CINC crisis planning staffs is also being altered by the worldwide explosion of information technologies. Information-sharing capabilities within and between US staffs have progressed far beyond those available only ten years ago. Many staff officers remember the agony inflicted by immature information systems during DESERT SHIELD/STORM. The difficulties of procedures such as dissemination of the Air Tasking Order or an important piece of imagery often seemed insurmountable. Today, these activities have become routine due to vastly better communications pipes, improved software and hardware, and greatly enlarged common user networks. For example, the maturation of the Global Command and Control System (GCCS) and its Secret-LAN communications backbone has transformed the ability of US planning staffs to coordinate and disseminate crisis planning documents. Access to intelligence materials for planning has been similarly improved by innovations such as Intelink (a vast classified information sharing system) and soft-copy map libraries. Even at the combined level, the development of multinational secure computer networks such as the NATO-standard CHRONOS system have eased communications problems for crisis planners.

These improvements in military connectivity are small, however, in comparison to the amazing scale and rapid pace of the communications revolution sweeping the civilian world. The emergence of the Internet as a dominant means of communication on the planet will have repercussions that are only beginning to be understood. Some projections estimate as many as one billion Internet users worldwide by the year 2005.⁴ Moreover, in contrast to current usage patterns, future Internet users will be more common in so-called underdeveloped countries.

⁴ Kitty Williams, "Internet Provides Kosovo Coverage," Web Pointers On-line, Available [On-line]: <<http://www.webpointers.com/kosovo.html>> [20 April 1999]

Cellular phone technology allows these nations to skip an entire generation of expensive hard-wired phone systems and move directly to digital wireless communications. Wireless data modems are already widely available for home computers. Together, these two technologies will effectively “wire” much of the developing world for the Internet in the near term. Even greater worldwide connectivity will be offered by satellite-based data transmission networks such as Teledesic.

The personal computer itself is on the verge of major transformation. A new generation of truly portable computers is already being tested with capabilities far beyond today’s rather clumsy laptops. For example, IBM has developed a computer small enough to be worn on the belt, complete with wireless modem and a miniature eyepiece to display information.⁵ When combined with other new developments such as voice recognition, faster processors, imbedded digital cameras, and improved data compression, these new computers will provide Internet access on demand, anywhere on the globe. Virtually anyone will be able to describe, record and share what is happening in front of them with the entire world. Thus, the development of a true “global infosphere” with unprecedented levels of transparency will occur -- and much sooner than one might think.

KOSOVO: THE FIRST INTERNET WAR

The initial effects of this new infosphere were already being felt during recent NATO combat operations in Kosovo. During the build up to the conflict, literally hundreds of new and existing Internet web sites with Kosovo-related information were identified. These ranged in complexity from simple chat rooms and bulletin boards to slick multimedia presentations. The

⁵ IBM Press Release, “Wired for Wear: IBM researchers demonstrate a wearable ThinkPad prototype” Available [On-line]: <http://www.ibm.com/news/1s/1998/09/jp_3.phtml> [23 April 1999]

information contained within these sites had no controls whatsoever on their content, thus leading to a tremendous amount of "noise" in the system. Although crackpot rants, propaganda and wild rumors were common, some sites were of real concern to US planners due to their potential impact on operational security (OPSEC).

One example was the web site run by the Federation of American Scientists (FAS). The FAS is dedicated to the dissemination of defense information gained through open source materials and freedom of information requests. Their site is a vast repository of accurate information on US military capabilities, plans and current operations. During Kosovo the FAS site contained accurate data on NATO orders of battle, intelligence collection capabilities and weapons characteristics. Ironically, some of this data was gleaned from DoD and NATO unclassified web sites.⁶

Another web site of concern was run by Skywatch, a UK-based tail watching group. Tail watchers, also called "plane spotters," are avid aerospace hobbyists who regularly haunt the perimeter fences of US and NATO airfields to gather and share aircraft data with fellow spotters. In recent years these groups have established several web sites to better share information with their peers. During Kosovo the Skywatch site posted details of a B-52 deployment to Britain including numbers, call signs, maintenance status and tail numbers. The site even included photos in which external weapons loads could be discerned.⁷

It is unknown whether the Yugoslavs were able to use this information or were even aware of it. Nonetheless, it is obvious that potential adversaries can use this type of Internet-

⁶ FAS Military Analysis Network, Available [On-line]: <<http://www.fas.org/man/dod-101/ops/kosovo>> [18 October 1999]

⁷ Skywatch Emergency Update Page, Available [On-line]: <<http://www.skywatch.dircon.co.uk>> [23 February 1999]

derived information to fill substantial gaps in their knowledge of US military capabilities and intentions. As more and more military-related sites appear on line, the Internet is rapidly becoming a vital source of intelligence data even for nations with formal intelligence collection systems. For those lesser-developed nations without worldwide collection assets, the Internet provides previously undreamed-of intelligence opportunities.

The Internet can also be used by adversary nations (and non-state actors) to disseminate propaganda and misinformation. During Kosovo there was a lively battle in cyberspace between pro-Albanian and pro-Serbian web sites. Hacking attacks against opposing web sites took place on several occasions, and even some "false flag" activities occurred. For example, the Belgrade-based opposition radio station B92 continued to broadcast anti-Milosevic stories via a Netherlands-base Internet service provider after it was forced off the airwaves by Serbian authorities. After several weeks of maneuvering, the Serbs were able to gain control of the B92 site address and began to use it to advance their own propaganda. Fortunately their tactics were crude (including an animation of President Clinton transforming into a chimp) and the deception was quickly discovered. A "Free B92" web site was quickly established and the two sites exchanged verbal broadsides throughout the remainder of the conflict.⁸

THE COMING CRUNCH

So what does all this mean to the poor crisis planners already working through the weekend for their regional CINC? The news is mixed. On the negative side, it seems a sure bet that the crisis planning workload is bound to increase. The combination of an engagement-oriented US foreign policy and an unstable global geopolitical situation will ensure that regional

⁸ Free B-92, Available [On-line]: <<http://www.freeb92.net>> [20 October 1999]

CINCs will have to handle large numbers of crises for the foreseeable future. Even absent a major regional conflict, the pressures of uneven economic development, population growth, weapons proliferation, ethnic hatreds and religious strife will generate endless contingencies which will require US military involvement. Increased attention by future US administrations to global issues such as the environment, disease and transnational crime will add to the crisis planning load.

At the same time, the planners' task will be made more complex by the multinational nature of almost all future military contingencies. Going a step beyond combined operations, these future contingencies will require close cooperation of not only national militaries and governments but a host of inter-governmental and non-governmental organizations as well. Again, the Kosovo conflict provides a valuable example of this trend. Even before the air campaign began, operating simultaneously on the ground in and around Kosovo were national militaries, an international refugee organization (the UN High Commission on Refugees), a regional security organization (the Organization for Security and Cooperation in Europe), an international criminal tribunal and a vast array of private charities and relief agencies. How will planners of future operations control, or at least keep track of, all these players?

On the technology side, there is also cause for concern. The emergence of the global infosphere will affect planning in several fundamental ways. First is the enormous amount of raw data which will become available on virtually any situation around the world. Unfortunately this unprecedented access to information does not equate to superior knowledge for planners. The totally unvetted nature of most information on the Internet plus its sheer volume pose significant problems. Few planners will have time to read, let alone cross-check and collate the information on dozens, if not hundreds, of web sites. Relying on the J-2 to fulfill this responsibility is unlikely

to be satisfactory, given that the intelligence staff is already fully employed monitoring classified collection means. Unless this problem can be solved, planning staffs run the risk of becoming saturated with a toxic level of raw data, thereby losing sight of critical information which may be key to mission success.

This surfeit of information poses a related problem for senior decision makers. Command paralysis may occur if the planning staff cannot screen the boss from the deluge of information which will arrive in his or her e-mail queue when a crisis erupts. Military executives are already reaching the saturation point in terms of the amount of reading material they can absorb. When added to the telephone, the daily video conference and CNN, the potential exists to seriously degrade crisis decision-making by choking senior leaders with a blizzard of information they cannot possibly handle. Additionally, senior military leaders cannot be seduced by the impression that the new infosphere will completely eliminate gaps in knowledge. Difficult military decisions will still have to be made based on imperfect intelligence.

Yet another effect of the infosphere will be a transformation in the current practice of OPSEC. In a world where virtually everyone with a personal computer is a potential intelligence collector (or media reporter), the idea of moving *any* significant military force without immediate public awareness may be obsolete. At the same time, the requirement to coordinate plans with multiple nations and organizations will make the crisis planning process itself increasingly transparent. The days when a CINC could create a "Black Hole" planning cell and expect to keep operational details restricted to a small group of specially-cleared individuals are past. Far too many people must be involved in the coordination process of any multinational operation to maintain stringent controls, and many outside observers can deduce military planning options from open source information alone. Moreover, an unhappy side-effect of current technology is

that any leak spreads uncontrollably. One example of this phenomenon is a recent embarrassing episode in which the classified Rules of Engagement for NATO forces in Kosovo appeared on the Internet.⁹

A final effect of the infosphere on crisis planners may be that of time compression. With pervasive and immediate media coverage of starvation, atrocities or natural disasters anywhere in the world, US political leadership will come under immense public pressure to "do something" almost immediately. Additionally, the realization that OPSEC is a fleeting commodity will put additional pressure on CINC's to execute quickly in order to preserve what advantage they can through tactical surprise. Although the political process and need for multinational cooperation may apply a brake to the process in some cases, CINC staffs should assume that the time available to conduct crisis planning will inevitably shrink. In any case, the crisis planning process needs to be streamlined in order to preserve the maximum amount of preparation time for the people who really need it -- the operators going in harm's way.

HOPE FOR THE FUTURE?

Thus far the picture seems bleak: a future of overworked, understaffed crisis planners trying to sift through mountains of useless data and coordinate a multinational circus -- while the CINC tries to make decisions in a fishbowl. All may not be lost, however. Several initiatives have already been taken to address the problem of over-tasked CINC planning staffs. The first of fix is the most obvious one -- rapid augmentation of CINC staffs during periods of crisis. Throughout the 1990s support organizations in CONUS have perfected the capability to rapidly deploy tailored teams of experts to any regional CINC who expresses a need. The intelligence

⁹ Adam Lusher and Sean Thomas, "NATO Kosovo Plan Leaked on Net," *London Sunday Telegraph*, 2 April 2000, p.1.

community has been particularly aggressive in this area. For example, during Kosovo not only did the national agencies such as CIA and DIA send teams forward, but also service intelligence arms such as the National Air Intelligence Center and the Naval Intelligence Support Center. Operations planners were similarly supported by teams from the Joint Warfare Analysis Center and the Air Force's CHECKMATE planning cell.

Crisis augmentation is not a panacea, however. National-level augmentation teams are valuable and rare assets and thus are hard to obtain for less than major contingencies. For the same reason, they are usually pulled back quickly once the immediate crisis has passed, leaving the CINC staff to handle the often drawn-out aftermath of a contingency operation. Of course, the CINC must feed, house, protect and provide workspace and communications for these personnel when they arrive. Moreover, travel time for these teams from the US to Germany or Hawaii is a significant factor and will be even more so in the future if time compression becomes a major problem as was suggested above.

The second fix is the concept of "*reach back*," which has become possible because of improved communications technology. Under this concept, augmentation teams are formed in CONUS, but they remain in home garrison and participate in the CINC planning process (or actual execution) via electronic means such as video conferencing, e-mail and computer chat windows. A high point in this process was reached during Kosovo with the activities of DGS-2, an Air Force ground unit which supports the U-2 aircraft. Although DGS-2 is designed to deploy in theater to provide near real time analysis of U-2 collection targets, during Kosovo it performed its mission from home base at Beale AFB, California. This was possible because of the existence of reliable, high-capacity satellite communications. Nonetheless, while it proved very successful,

this arrangement was initially a very hard sell to both the CINC and the Air Force component commander.

Their skepticism was not misplaced; it highlighted some of the major problems with *reach back*. Some critics of *reach back* focus on the communications technology involved, emphasizing the possibility of a communications failure greatly impacting operational capabilities. While this argument is still a concern, the US is already so dependent on high-capacity satellite communications that any major failure would severely impact all US military operations, whether based in theater or not. Long-haul pipes which run back to CONUS are no more vulnerable or failure-prone than those supporting units in theater. A better argument against *reach back* can be made by emphasizing the value of human interaction, especially in crisis planning. CINCs always prefer to have their key planning assets forward, and for good reason. A memorandum of understanding or a video conference is no substitute for an unhappy four-star poking a planner in the chest as a motivational tool -- or as an aid to clear communication. At a more basic level, the crisis planning process depends greatly on a group of human beings exchanging ideas in physical proximity. The "gaggle around the map" remains by far the best mechanism for brainstorming a problem and testing ideas quickly. Electronic connectivity necessarily inserts filters into this natural process and degrades it.

A third fix is the simplification wherever possible of the planning process. One recent development which may prove a boon to planners is the revolt against overdone presentation graphics led by the Chairman of the Joint Chiefs of Staff himself.¹⁰ This healthy trend could save much preparation time for crisis planners -- if it can be enforced beyond the Washington, DC,

¹⁰ Greg Jaffe, "What's Your Point, Lieutenant? Just Cut to the Pie Charts," *The Wall Street Journal*, 26 April 2000, p.A1.

area. Any improvements of this sort which streamline the planning process should be eagerly embraced by CINC staffs as they try to deal with an ever-growing workload.

Another area where a minor change in command philosophy could reap benefits is the problem of crisis action teams (CATs) which are maintained beyond their useful life spans. (In that respect, CATs are like Windows programs on a computer. Even though they're no longer on the screen, they're still running in the background and using up memory.) Even when drastically scaled back, CATs involved in post-crisis monitoring functions are doing a mission that is already being done as well (and cheaper) by the CINC's full-time watch organization. Instead of treating CATs as normal adjuncts to the staff, CINCs and J-3s must view them as temporary burdens which exact a steep cost on normal staff functions and personnel. They must be just as proactive in closing down crisis teams as they are in forming them, or else they risk attriting their staff to the point where it is unable to handle a new emergency.

The problem of transparency is an even thornier issue which has yet to be effectively addressed. The OPSEC problem is growing worse every day, driven by the twin issues of emerging communications technology and the mandate to conduct almost all operations under a multinational banner. However, the end result of this phenomenon may be less severe than one would expect. One justification for this argument is the very scale of the problem and the enormous amount of noise in the system. Just as US planners will be struggling with information overload, so will the adversary. Low-tech adversaries will be especially "deaf" to Internet-based information as they will probably lack the experience and amount of analytical assets which will be needed to effectively monitor the cyber environment. It may be nearly impossible for them to discern critical US operational details until it is too late to react, especially if crisis plans retain sufficient flexibility to offer multiple employment options. US deception operations could add to

enemy confusion, although caution is needed in order to satisfy legal, ethical and practical requirements. For example, how could deception planners insure that an active Internet disinformation campaign would be received by the adversary? If discovered, what damage would the exposure of such a campaign do to world opinion toward the US position?

A second argument against the danger of transparency is a general philosophical one. Assuming that future adversaries will represent less democratic and open societies than the US, they have much more to fear from the infosphere. Regimes which rely on the strict control of information to maintain themselves in power can ill afford to give their people or even their security agencies wide access to the Internet and its host of dangerous ideas. Repressive governments which attempt to use the Internet as a collection tool or means of propaganda may find that they have opened Pandora's box. Open societies by their very nature are better equipped for this aspect of the future and thus should actually welcome transparency as a potential force multiplier.

NO EASY SOLUTIONS

No doubt by this point the reader is waiting for the new technological insight, miraculous staffing plan, or revolutionary strategy proposal which will solve all the problems listed above and make life good for the CINC crisis planners. Unfortunately, no such easy solutions exist. Barring a radical disengagement of the US from world affairs or the sudden outbreak of global peace and harmony, the regional CINCs will remain very busy. Technological advances will assist crisis planners in some respects, but will pose new challenges as well. The reality is that tomorrow's CINC crisis planners will be worked harder and stretched thinner than ever before. Unless some creative means are found to ease this growing burden, it will become unsustainable. The crisis

planning process will fail. In the best case, that failure will manifest itself in burned-out personnel and lost opportunities. In the worst case, planning failure will result in national embarrassment and unnecessary casualties.

This grim scenario is not pre-ordained. CINCs and their staffs should continue to work hard to improve the crisis planning process. Incremental gains are valuable and may well prove the margin between success and failure. Augmentation, *reach back* and simplification will not solve over-tasking, but they may ease the burden. It remains to be seen what impact the Internet and future technologies will have -- but they should be looked upon as tools, rather than threats.

Finally, there is value in simply alerting the senior leadership to the coming crunch in the crisis planning business. CINCs must be sensitized to the increasing problems in workload and manning, as well as the looming issues of the infosphere environment. With command attention on the problem, the funding and creative solutions needed to address these problems will be found. Our crisis planners must have this support in order to meet the challenges of the new millennium.

BIBLIOGRAPHY

Barry, Charles. "NATO's Combined Joint task Forces in Theory and Practice," Survival, Spring 1996, 81-97.

Chelberg, Robert, Jack Ellertson, and David Shelley. "EUCOM - At the Center of the Vortex." Field Artillery, October 1993, 12-16.

Cooke, Thomas. "NATO CJTF Doctrine: The Naked Emperor." Parameters, Winter 1998-99, 124-136.

FAS Military Analysis Network, <<http://www.fas.org/man/dod-101/ops/kosovo>> (18 October 1999).

Free B-92, <<http://www.freeb92.net>> (20 October 1999).

Gellman, Barton. "AIDS Declared Threat to Security." The Washington Post, 30 April 2000, A1.

IBM Press Release, "Wired for Wear: IBM researchers demonstrate a wearable ThinkPad prototype." IBM Press Release, <http://www.ibm.com/news/1s/1998/09/jp_3.phtml> (23 April 1999).

Jaffe, Greg. "What's Your Point, Lieutenant? Just Cut to the Pie Charts." The Wall Street Journal, 26 April 2000, A1.

Lusher, Adam and Sean Thomas. "NATO Kosovo Plan Leaked on Net." London Sunday Telegraph, 2 April 2000, 1.

Skywatch Emergency Update Page, <<http://www.skywatch.dircon.co.uk>> (23 February 1999).

U.S. Air Force Personnel Center. Update briefing, Langley AFB, Virginia, 20 March 1999.

U.S. President, A National Security Strategy for a New Century. Washington: U.S. Govt. Print. Off., 1999.

U.S. Joint Chiefs of Staff, Doctrine for Planning Joint Operations. Joint Publication 5-0. Washington 1995.

Williams, Kitty. "Internet Provides Kosovo Coverage." Web Pointers On-line, <<http://www.webpointers.com/kosovo.html>> (20 April 1999).